

### **Amendments to the Claims**

1 – 25. (Cancelled)

26. (New) A process for modifying an application computer program that includes a plurality of subsections having boundaries, said application computer program configured to run under the control of an operating system, said process steps comprising:

substituting an operating system instruction that causes an interrupt for one or more bytes of at least one subsection;

relocating the substituted bytes to a location in the application computer program that is distinct from the boundaries of the subsection; and

adding an execution controller computer program into the application computer program; where the execution controller computer program is configured to be launched by the application computer program, and where the execution controller computer program, once launched, uses an operating system debugger interface to attach the execution controller computer program to the application computer program and restores the operating system instruction that causes an interrupt with the substituted bytes.

27. (New) The process of claim 26, further comprising the step of:

identifying the boundaries of the at least one subsection.

28. (New) The process of claim 27, where one of the boundaries is a flow control instruction.

29. (New) The process of claim 26, further comprising the step of: encrypting at least a portion of at least one subsection.

30. (New) The process of claim 29, further comprising the step of:

adding information used to decrypt the encrypted portion to the application computer program.

31. (New) The process of claim 26, further comprising the step of:  
adding tamper detection instructions and data to the application computer program file.
32. (New) A process for executing an application computer program defining a plurality of subsections, said application computer program configured to run under the control of an operating system and incorporating an execution controller computer program, said process steps comprising:  
launching the application computer program;  
launching the execution controller computer program, where the execution controller computer program is launched by the application computer program;  
attaching the execution controller computer program to the application computer program using the operating system debugger interface; and  
executing the application computer program until an operating system instruction that causes an interrupt is encountered.
33. (New) The process of claim 32, further comprising the step of:  
after an operating system instruction that causes an interrupt is encountered, resuming execution of the application computer program.
34. (New) The process of claim 32, further comprising the step of:  
after an operating system instruction that causes an interrupt is encountered, terminating the execution of the application computer program.
35. (New) The process of claim 32, further comprising the steps of:  
substituting an operating system instruction that causes an interrupt for one or more bytes of at least one subsection;  
after an operating system instruction that causes an interrupt is encountered, restoring the

operating system instruction that causes an interrupt with the substituted bytes; and

resuming execution of the application computer program, starting at the restored bytes.

36. (New) The process of claim 32, further comprising the step of:

after an operating system instruction that causes an interrupt is encountered, authorizing a continued execution of the application computer program.

37. (New) The process of claim 36, where the step of authorizing a continued execution of the application computer program comprises authenticating a user of the application computer program.

38. (New) The process of claim 32, where at least a portion of the at least one subsection has been encrypted, further comprising the steps of:

after an operating system instruction that causes an interrupt is encountered, decrypting the encrypted portion; and

executing the decrypted subsection.

39. (New) The process of claim 38, further comprising the step of:

re-encrypting the decrypted subsection.

40. (New) The process of claim 38, where at least a portion of the information used to decrypt the encrypted portion is obtained from a key server computer program.

41. (New) The process of claim 38, where at least a portion of the information used to decrypt the encrypted portion is obtained from a location in the application computer program.

42. (New) The process of claim 32, further comprising the steps of:

after an operating system instruction that causes an interrupt is encountered, detecting if there has been tampering of the application computer program; and

if tampering has been detected, reporting information related to the tampering to a user of

the application computer program.

43. (New) The process of claim 32, further comprising the steps of:

after an operating system instruction that causes an interrupt is encountered, detecting if there has been tampering of the application computer program; and

if tampering has not been detected, resuming execution of the application computer program.

44. (New) A process for executing an application computer program that includes a plurality of subsections having boundaries, said application computer program configured to run under the control of an operating system, said process steps comprising:

substituting an operating system instruction that causes an interrupt for one or more bytes of at least one subsection;

relocating the substituted bytes to a location in the application computer program this is distinct from the boundaries of the subsection;

adding an execution controller computer program into the application computer program;

launching the application computer program;

launching the execution controller computer program, where the execution controller computer program is launched by the application computer program;

attaching the execution controller computer program to the application computer program using the operating system debugger interface;

executing the application computer program until an operating system instruction that causes an interrupt is encountered;

after an operating system instruction that causes an interrupt is encountered, restoring the operating system instruction that causes an interrupt with the substituted bytes; and

resuming execution of the application computer program, starting at the restored bytes.

45. (New) The process of claim 44, further comprising the steps of:

encrypting at least a portion of at least one subsection of the application computer program; and

after an operating system instruction that causes an interrupt is encountered, decrypting the encrypted portion.

46. (New) The process of claim 44, further comprising the steps of:

adding tamper detection instructions and data into the application computer program;

after an operating system instruction that causes an interrupt is encountered, detecting if there has been tampering of the application computer program; and

if tampering has been detected, terminating the execution of the application computer program.

47. (New) The process of claim 44, further comprising the steps of:

adding tamper detection instructions into the application computer program;

after an operating system instruction that causes an interrupt is encountered, detecting if there has been tampering of the application computer program; and

if tampering has been detected, reporting the tampering to a user of the application computer program.

48. (New) The process of claim 44, further comprising the steps of:

after an operating system instruction that causes an interrupt is encountered, authenticating a user of the application computer program; and

if the user of the application computer program is authenticated, resuming the execution of the application computer program.

49. (New) The process of claim 44, further comprising the steps of:
- after an operating system instruction that causes an interrupt is encountered,
- authenticating a user of the application computer program; and
- if the user of the application computer program is not authenticated, terminating the execution of the application computer program.